Bibliographic data: CN 1147738 (A)

Fireproof wall system

Publication date:	1997-04-16
Inventor(s):	WU SHIZHONG [CN] +
Applicant(s):	TIANRONGXIN TECHNOLOGY & TRADE [CN] +
Classification:	**- international:** ***H04L29/02; H04L29/06; H04L29/08;*** (IPC1-7): H04L29/02 **- European:**
Application number:	CN19961009573 19960902
Priority number(s):	CN19961009573 19960902

Also published as:

- CN 1075695 (C)

Abstract of CN 1147738 (A)

The present invention consists of five parts including safety controller, system controller, router, safety card and safety card vise managing system, and it is mounted between outer internet and inside net. The present system can protect interior resource against damage from illegal access and prevent interior data from outputting. It isolates the inside net and outer internet and performs safety inspection to the connection or data from and to the inside net based on the safety regulations set by the system, so as to raise the safety of inside net.

[19]中华人民共和国专利局

[51]Int.Cl[6]
H04L 29/02

[12] 发明专利申请公开说明书

[21] 申请号 96109573.3

[43]公开日 1997 年 4 月 16 日

[11] 公开号 CN 1147738A

[22]申请日 96.9.2

[71]申请人 北京天融信技贸有限责任公司

地址 100080北京市2704信箱三信时代信息公司转

[72]发明人 吴世忠

权利要求书 2 页 说明书 7 页 附图页数 3 页

[54]发明名称 防火墙系统

[57]摘要

本发明由安全管理器、系统管理器、路由器、安全卡和安全卡签证机关管理系统五部分组成，它安置于外部 Internet 与内部网络之间。本系统可以保护内部资源不被非法访问的破坏，阻止内部未经发布和授权的信息输出。它隔离内部网与外部 Internet 网的直接连接，并可根据系统设置的安全规则对进、出内部网络的连接或信息进行安全检查，从而提高了内部网络的安全性。

权　利　要　求　书

1.一种防火墙系统，其特征在于，

(1) 它由安全管理器、系统管理器、路由器、安全卡及安全卡签证机关管理系统五部分组成；

(2) 它安置在信息提供者或内部网络或专用网络与外部国际互连网之间；

(3) 它采用具有分组过滤功能的路由器与外部网络连接，路由器根据配置的安全规则对进出数据进行控制；

(4) 它通过系统管理器实现系统配置，系统管理器在得到安全管理器的授权后执行系统配置；

(5) 它由安全管理器提供系统配置的授权鉴别，安全管理器的授权鉴别由安全卡等确认，安全卡由安全卡签证机关管理系统生成和管理。

2.根据权利要求 1 所述的系统，其特征在于，

(1) 安全管理器由通信控制模块、中央控制模块、输入/输出控制模块、安全控制模块和安全卡鉴别模块等构成；

(2) 安全管理器利用安全卡鉴别模块识别安全卡；

(3) 安全管理器通过其通信控制模块与系统管理器、路由器连接，通信控制模块采用 RS232 接口分别与系统管理器和路由器相连；

(4) 安全管理器提供系统管理器系统配置时的授权鉴别。

3.根据权利要求 1 所述系统的系统管理器，其特征在于，

(1) 它由一台 386 以上微机或专用微机或工作站和一套系统管理软件构成，软件运行环境为视窗；

(2) 它由 RS232 口与安全管理器连接；

(3) 它经由安全管理器与路由器的控制口相连，提供对系统的菜单式管理，执行防火墙系统配置和安全规则配置，并收集审计信息；

(4) 系统管理软件由过滤规则编辑器、防火墙状态监测器、控制列表监测器和告警信息收集器等功能模块构成；

(5) 它在执行网络安全政策配置时，必须得到安全管理器的授权。

4.根据权利要求 1 所述的系统，其特征在于，

(1) 安全卡是一个具有存贮与处理功能的智能卡，卡内存放着持卡者的安全证书；

(2) 安全卡安全证书的生成和管理由独立的安全卡签证机关管理系统实现；

(3) 安全卡签证机关管理系统由一台 386 以上微机和一套专用管理软件构成。

5.根据权利要求 1 所述系统安全管理器的程序流程，其特征在于，

(1) 安全管理器的通信控制模块不断截获来自两端的通信数据，加以判定后进行传送，同时也可以直接向路由器发送命令收集信息和数据；

(2) 对来自系统管理器的数据，安全管理器依照存放在安全控制模块中表内的数据进行比较判断，实施分级别的安全控制，一旦判定需要特别授权和进行合法认定时，便要求用户插入安全卡并正确地输入 标识身份的个人识别号码；

(3) 同时安全管理器对来自路由器和系统管理器的数据进行必要的记录和转贮，根据防火墙的运行状态，安全管理器提供自身所处工作状态提示，并辅以“ 正常”、“ 错误”和“ 告警”三种状态的液晶显示；

(4) 当发现防火墙的配置文件可能被修改时，安全管理器发出声音报警，提醒系统安全管理员进行确认。

说　　明　　书

防火墙系统

本发明涉及国际互连网(Internet)的网络安全防火墙技术，它属于计算机网络安全技术。

防火墙(firewall)这一概念引入国际互连网安全方面最早是在1993年。现有的最接近本发明的技术是具有分组过滤功能的防火墙，如目前世界市场占有率最高的CheckPoint公司的FireWall-1产品，(见FireWalls for Sale,BYTE，Vol.20,No.4,1995,P.99)。这种防火墙系统自身不具备较强的防护能力，无法识别操作者身份，并且防火墙本身及网络用户的合法性也不能得到鉴别，网络安全政策往往不能在技术手段上得到保证，因此不适合中国的国情。

本发明的目的在于：提供一种由安全卡、安全卡签证机关管理系统进行内部网络安全保护及用户管理，能有效实现网络安全政策，具有分组过滤功能的防火墙系统。

本发明的任务是以下述方式完成的：本系统是由安全管理器、系统管理器、路由器、安全卡及安全卡签证机关管理系统五部分组成。路由器根据配置的安全规则执行进出数据的控制，系统管理器在得到安全管理器的授权后执行本防火墙的预配置和安全政策配置(统称为系统配置)，安全管理器的授权鉴别由安全卡和个人识别号码确认，安全卡由安全卡签证机关管理系统生成和管理。

本发明安置于信息提供者或者内部(专用)网络和外部Internet之间，可以保护内部资源不被非法访问和破坏，阻止内部未经发布和授权的信息输出。它可作为内部网络与Internet之间的安全路由器，采用硬件方式实现，处理速度极快。该防火墙经过防篡设计，采用目前成熟的分组过滤技术实现对内、外网络之间数据流动的控制，通过安全卡技术实现对防火墙系统本身的安全保护和管理。

安全管理器由中央控制模块、输入/输出控制模块、安全控制模块、安全卡鉴别模块和通信控制模块等构成，它通过通信控制模块与系统管理器、路由器连接。它是本发明的关键部分，它将路由器的控制(Console)端口与系统管理器(终端)隔离开来，一是避免了终端直接从控制端口对网络安全规则进行配置，二是担负着对来自系统管理器的合法性确认和特别授权鉴别，三是实施分级安全控制和收集审计信息。这就从技术上提供了对用户单位网络安全规则配置的强制性约束手段，同时达到保护用户单位内部网络资源安全的目的。

安全管理器的基本工作原理是，其通信控制模块不断截获来自两端的通信数据，加以判定后进行传送，同时也可以直接向路由器发送命令收集信息和数据。对来自系统管理器的数据(命令)，它依照存放在安全控制模块中表内的数据进行比较判断，实施分级别的安全控制，一旦判定需要特别授权和进行合法认定时，便要求用户插入安全卡并正确地输入 标识身份的个人识别号码(PIN)数据。同时它对来自路由器和系统管理器的数据(信息)进行必要的记录和转贮，根据防火墙的运行状态，安全管理器提供自身所处工作状态提示，并辅以“ 正常”、“ 错误”和“ 告警”三种状态的液晶显示。当发现防火墙的配置文件可能被修改时，发出声音报警，提醒系统安全管理员进行确认。安全管理器的程序流程将在后面的附图中加以说明。

安全管理器通过RS232接口分别与系统管理器和路由器相连，提供控制台(系统管理器)与路由器的通信连接，对控制台配置路由器安全规则的附加授权机制进行管理，记录安全管理器的使用情况、故障情况以及收集来自路由器的参数和数据，并将这些数据分类存贮或传送到控制台。

安全管理器在针对系统资源配置和安全规则设置进行操作时，利用声光报警提示当前的操作类型。在试图进入安全状态及进入安全状态后，除安全管理全开放外，系统将自动记录下所有的有关安全命令的操作，以及该操作执行的日期、时间，由此文件可以追踪一段时间以来的所有有关的安全操作。对于可能的对系统资源的配置或安全规则的设置的修改行为，系统通过存储下来的原始安全规则与新的安全规则进行比较，可以及时发现违规的事件，对某些违规事件参照预先存放的基本安全准则及时自动进行 更正，并立即对违规事件进行详细的记录，包括：违规的事件、违规的安全命令，同时利用安全管理器的声光报警提醒操作人员可能有重大错误。

路由器可以是世界上任一种具分组过滤功能的产品。本发明样机采用的是美国Cisco公司的Cisco 2501产品，它提供路由选择和分组过滤功能，按照控制台配置的安全规则完成对进出内部网络信息的过滤控制。也可以在已有分组过滤路由器的用户中，加装安全管理器和系统管理器等装置构成本发明系统；还可以把路由器集成到安全管理器中，这些均是本发明的一些非限定实施特例，并不影响本发明的一般性。

系统管理器是由一台386以上微机或专用PC机和一个具有先进的图形用户界面(GUI)功能的系统管理软件组成，运行在视窗(Windows)环境下。软件要求：操作系统为DOS5.0或更新版本，运行环境要求为中文Windows3.1或更新版本，或者英文Windows3.0或更新版本(在英文Windows上需加载中文之星或其它汉字平台软件)。硬件要求：IBM或IBM兼容机(80386DX处理器，4M内存，一个软驱，一个

控制用串行口，一个鼠标接口)，最小剩余硬盘空间20M。建议使用80486DX以上计算机，8M以上内存，420M以上硬盘。

系统管理软件由过滤规则编辑器、防火墙状态监测器、控制列表监测器和告警信息收集器等功能模块构成，存贮在硬盘上。

系统管理器经由安全管理器与路由器的控制口相连，提供对系统的菜单式管理和防火墙系统配置以及安全规则配置，并收集审计信息。

系统管理器用于配置整个网络的安全政策，控制与监测防火墙的运行，观测登录与告警信息。

本发明可根据不同安全要求，使用不同的安全规则进行配置。我们将为保证网络安全所需的基本配置称为预配置。预配置是构建防火墙的基础条件，用户在进行路由器系统配置时必须将预配置参数加到用户的配置文件中。系统管理软件提供的“系统配置文件确认”程序将本发明提供的预配置参数与用户配置的运行参数进行比较，确认其配置是否合法。

防火墙安全规则配置文件存放在路由器的NVRAM中，它是防火墙“允许/禁止”连接或访问控制的依据，控制这一配置权实际上就掌握了网络安全控制的决定权。为此采取了如下措施：(1)将路由器的AUX后备命令口利用预配置将其配置成异步通信(dedicated mode)方式，这就禁止终端直接从这个口登录到路由器；(2)通过对路由器各通信端口(含AUX口)的预配置禁止所有内部和外部用户从网络上登录到路由器，并加强进入路由器特权操作状态的口令、身份认定的管理。从而，对防火墙的配置权便集中到路由器的console端口，console端口直接与安全管理器连接，再通过安全管理器连到系统管理器。

系统安全管理员通过终端利用本发明的系统管理软件必须经由安全管理器才能对防火墙的系统进行配置，否则安全管理器将拒绝传送信息。系统安全管理员在对防火墙中涉及网络安全控制参数进行配置时，必须向防火墙前面板的“安全卡读入器”口插入安全卡，并输入正确的个人身份识别号码(PIN)，才能进入配置状态，否则防火墙的安全管理器将拒绝执行。

本发明自身的安全由安全卡及其管理系统来实施保护。安全卡是具有存贮和处理功能的智能卡(Smart卡)，智能卡是包含存贮器的微机芯片，其尺寸与信用卡相同，是一种可实时处理加密算法的有源器件。该技术属公知技术，它的安全性由于多功能、易替换、智能化等优点而得到极大提高。安全卡由防火墙安全人员保管并使用。安全卡内存放着持卡者的安全证书，这种安全证书的生成与管理是由专门的机构利用先进的密码学技术来实现的，这种机构称为“签证机关(CA)”。它的作用是：(1)为防火墙用户及管理者提供安全卡鉴别工具；(2)维护鉴别安全卡中的数据项；(3)更改安全卡的权限及级别；(4)颁发安全卡及生成PIN(个

人识别号码)；(5)维护安全卡的校验器。

一个防火墙有一张安全卡，安全卡的合法性、有效性、安全内容等由一个专门的安全卡签证机关管理系统(CAMS)来签发。安全卡签证机关管理系统是整个防火墙系统的有机组成部分，但由国家有关部门(或大型用户系统的领导部门)管理。只有持有安全卡，并拥有持有人的个人识别号码(PIN)，才能对本防火墙进行安全政策实施、更改等一系列操作。

安全卡签证机关管理系统(CAMS)是一个在网络环境(多防火墙构成的互联环境)下对多个安全卡进行核发、认证、识别、维护与管理的系统，它给每一张安全卡发放一个证书。该系统由国家或各级政府主管防火墙政策的部门控制，以保证安全卡的合法性和权威性。

该签证机关管理系统由一台386以上的微机和一套专门开发的管理软件构成，其安全证书的发放可以是脱机方式(单防火墙时)，也可以是联机方式(网络环境下)。签证机关管理系统生成的安全卡主要用于用户秘密信息的安全存贮。它按照防火墙安全应用所使用 的格式对卡进行初始化。然后将用于安全服务的有关信息装入格式化后的安全卡。

安全卡的作用主要是机密数据的安全存放和防火墙措施的安全处理。安全处理功能能够防止外部攻击者对安全政策实现过程的跟踪攻击，安全存放功能则能够防止非授权的读、写操作。在防火墙应用中，由于基于密码技术的安全参数很难被用户记忆，因此就采用安全卡来存贮。

在使用时，用户必须拥有自己的个人识别号码来激活安全卡。这样，即使安全管理人员在配置防火墙时也必须拥有安全卡，并用所知的个人识别号码来激活安全卡，从而达到对安全政策以及本防火墙自身的有效保护。

这种基于安全政策保护核心机密数据的安全逻辑分为下面两种：

(1)使用安全政策，以便获得授权来配置和修改防火墙中的核心工作参数。这种情况要求必须使用安全卡来进行，否则，安全模块将拒绝请求。

(2)不使用安全政策，无论使用安全卡与否，安全模块都允许访问防火墙。但是，用户的授权只许可“读”操作，任何“写”操作将被拒绝。

为了强化安全管理，本系统提供配置防火墙参数的一特别授权机制。传输控制协议/网际协议(TCP/IP)是Internet的通信协议，故而与之连接的计算机和网络都必须安装相应的TCP/IP协议。根据TCP/IP协议，传输的任何数据(应用层数据)都必须分割成若干小的数据报(datagram)，每个数据报经过传输层、IP层和网络存取层封装后再通过物理层进行传输。数据封装是指应用层的数据通过下面各层时，每层都将自己特有的报头加在收到数据段前面，再送到下一层的过程。对分组过滤有用的主要是传输层的报头和IP层的报头。TCP/IP格式是公知的，每个数据包

都包含有IP源地址、IP目的地址、协议类型、源端口号和目的端口号等特定信息。分组过滤就是利用这些特定信息和由路由器确定的路由信息，控制防火墙阻止或允许某些分组通过。

本发明是通过独占“安全规则设置权”技术以及附加安全控制授权机制，实现对网络系统资源配置和安全规则设置的严密而可靠的控制以及监审。在系统中，涉及安全的参数设置、安全规则设置及其变更必须通过安全审计。本发明的安全审计有一般管理级、管理员级和安全管理级等三级。进入安全管理级，需要持有合法的安全卡和输入正确的安全卡通行字。

本发明系统是基于分组过滤技术的网络安全控制系统，它按照用户设定的安全规则，对进、出分组逐一进行安全性检查分析，保障符合安全条件的分组信息畅通无阻，阻止不符合安全条件的分组信息通过，从而保证内部网络的安全。因此安全规则的正确配置是保证网络安全的关键。

安全规则的配置是为了阻止对内部网络可能的攻击，本发明在出厂时没有进行安全规则配置，缺省允许网络上 任何信息自由进出，即它只具备路由选择功能，防火墙功能有待用户根据具体政策进行适当的安全规则配置后，才能达到保护内部网络安全之目的。本发明可根据不同安全要求，使用不同的安全规则进行配置。本发明还配备有保证网络安全所需的基本配置，即预配置。系统管理软件提供的“系统配置文件确认”程序将本发明的预配置参数与用户配置的运行参数进行比较，确认其配置是否合法。

本系统的使用，除满足电气产品所需要的条件外，还应特别注意安全环境，必须有一定的防火、防窃、防洪和防尘等措施，气候潮湿的地方，应考虑除湿设备；气候干燥的地方应考虑防静电措施。

本发明的特征在于：本系统由安全管理器、系统管理器、路由器、安全卡和安全卡签证机关管理系统五部分构成。路由器根据配置的安全规则执行进出数据的控制，系统管理器在得到安全管理器的授权后执行本防火墙的预配置和安全政策配置(统称为系统配置)，安全管理器的授权鉴别由安全卡和个人识别号码确认，安全卡由安全卡签证机关管理系统生成和管理。

本发明安置于国际互联网信息提供者或者内部网络或者专用网络和外部网络之间。本发明采用公知的分组过滤技术，其工作原理是根据配置的安全规则，对进/出分组的源/宿地址或端口以及相应的控制协议进行判决，决定进/出分组“允许/禁止”通过并做出相应的路由选择。

安全管理器由中央控制模块、输入/输出控制模块、安全控制模块、安全卡鉴别模块和通信控制模块等构成，它通过通信控制模块与系统管理器、路由器连接。

安全管理器的基本工作原理是，其通信控制模块不断截获来自两端的通信数据，加以判定后进行传送，同时也可以直接向路由器发送命令收集信息和数据，对来自系统管理器的数据(命令)，它依照存放在安全控制模块中表内的数据进行比较判断，实施分级别的安全控制，一旦判定需要特别授权和进行合法认定时，便要求用户插入安全卡并正确地输入 标识身份的个人识别号码(PIN)数据。同时它对来自路由器和系统管理器的数据(信息)进行必要的记录和转贮，根据防火墙的运行状态，安全管理器提供自身所处工作状态提示，并辅以“ 正常”、“ 错误”和“ 告警”三种状态的液晶显示。当发现防火墙的配置文件可能被修改时，发出声音报警，提醒系统安全管理员进行确认。

系统管理器是由一台386以上微机或专用PC机和一个具有先进的图形用户界面(GUI)功能的系统管理软件组成，运行在Windows环境下。软件要求：操作系统为DOS5.0或更新版本，运行环境要求为中文Windows3.1或更新版本，或者英文Windows3.0或更新版本(在英文Windows上需加载中文之星或其它汉字平台软件)。硬件要求：IBM或IBM兼容机(80386DX处理器，4M内存，一个软驱，一个控制用串行口，一个鼠标接口)，最小剩余硬盘空间20M。建议使用80486DX以上计算机，8M以上内存，420M以上硬盘。

系统管理软件由过滤规则编辑器、防火墙状态监测器、控制列表监测器和告警信息收集器等各个功能模块构成，并存贮在硬盘中。

系统管理器经由安全管理器与路由器的控制口相连，提供对系统的菜单式管理和防火墙系统配置以及安全规则配置，并收集审计信息。

路由器可采用目前世界市场上较常见的各种具分组过滤功能的路由器产品。也可以在已有分组过滤路由器的用户中，加装安全管理器和系统管理器等装置构成本发明系统；还可以把路由器集成到安全管理器中，这些均是本发明的一些特例，并不影响本发明的一般性。

本发明是通过独占“ 安全规则设置权”技术以及附加安全控制授权机制，实现对网络系统资源配置和安全规则设置的严密而可靠的控制以及监审。在系统中，涉及安全的参数设置、安全规则设置及其变更必须通过安全审计。本发明的安全审计有一般管理级、管理员级和安全管理级等三级。进入安全管理级，需要持有合法的安全卡和输入正确的安全卡通行字。

安全管理器通过RS232接口分别与系统管理器和路由器相连，提供控制台与路由器的通信连接，对控制台配置路由器安全规则的附加授权机制进行管理，记录安全管理器的使用情况、故障情况以及收集来自路由器的参数和数据，并将这些数据分类存贮或传送到控制台。

安全管理器将会在针对系统资源配置和安全规则设置进行操作时，利用声光

报警提示当前的操作类型。在试图进入安全状态及进入安全状态后，除安全管理全开放外，系统将自动记录下所有的有关安全命令的操作，以及该操作执行的日期、时间，由此文件可以追踪一段时间以来的所有有关的安全操作。对于可能的对系统资源的配置或安全规则的设置的修改行为，系统通过存储下来的原始安全规则与新的安全规则进行比较，可以及时发现违规的事件，对某些违规事件参照预先存放的基本安全准则及时自动进行 更正，并立即对违规事件进行详细的记录，包括：违规的事件、违规的安全命令，同时利用安全管理器的声光报警提醒操作人员可能有重大错误。

下面结合附图对本发明做进一步的说明。

图1是本发明在Internet网中的位置图。它安装在内部网络与外部Internet之间，可以保护内部资源不被非法访问和破坏，阻止内部未经发布和授权的信息输出。过滤路由器是一台Cisco公司的Cisco 2501产品，它提供路由选择和分组过滤功能，按照控制台配置的安全规则完成对进出内部网络信息的过滤控制。

图2是本发明的结构框图。安全卡插入读卡器，并在终端输入正确的PIN，经中央控制模块处理确认授权后，系统管理器就具备了系统配置的权利，然后通过I/O控制模块输出LED显示信息，并可对路由器进行配置。

图3是本发明安全管理器实现框图。安全管理器的安全卡鉴别模块由一台Bull CP8读卡器构成，它通过RS232口与安全控制模块连接，中央控制模块由一台CPU(80486)加部分存贮器件组成，输入/输出控制模块由8255片构成，安全控制模块和通信控制模块的软件程序在中央控制模块中处理，通信控制模块与系统管理器和路由器的连接均采用RS232口。

图4是本发明安全管理器的程序流程图。

说　明　书　附　图

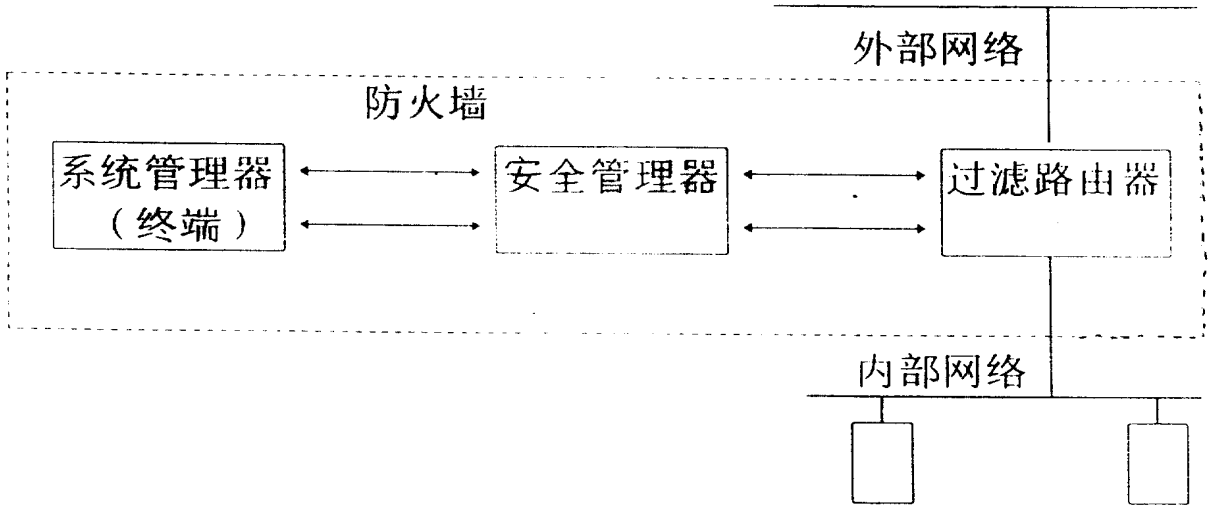

图1是本发明在Internet网中的位置图

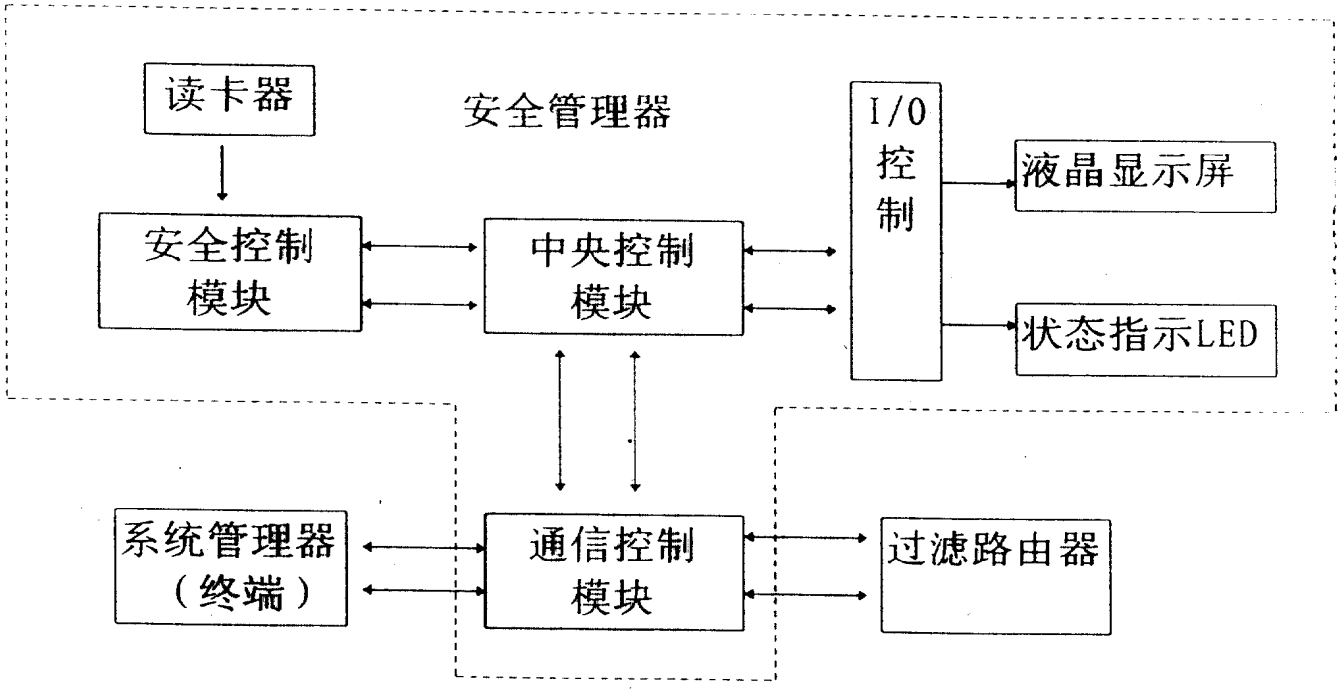

图2是本发明的结构框图

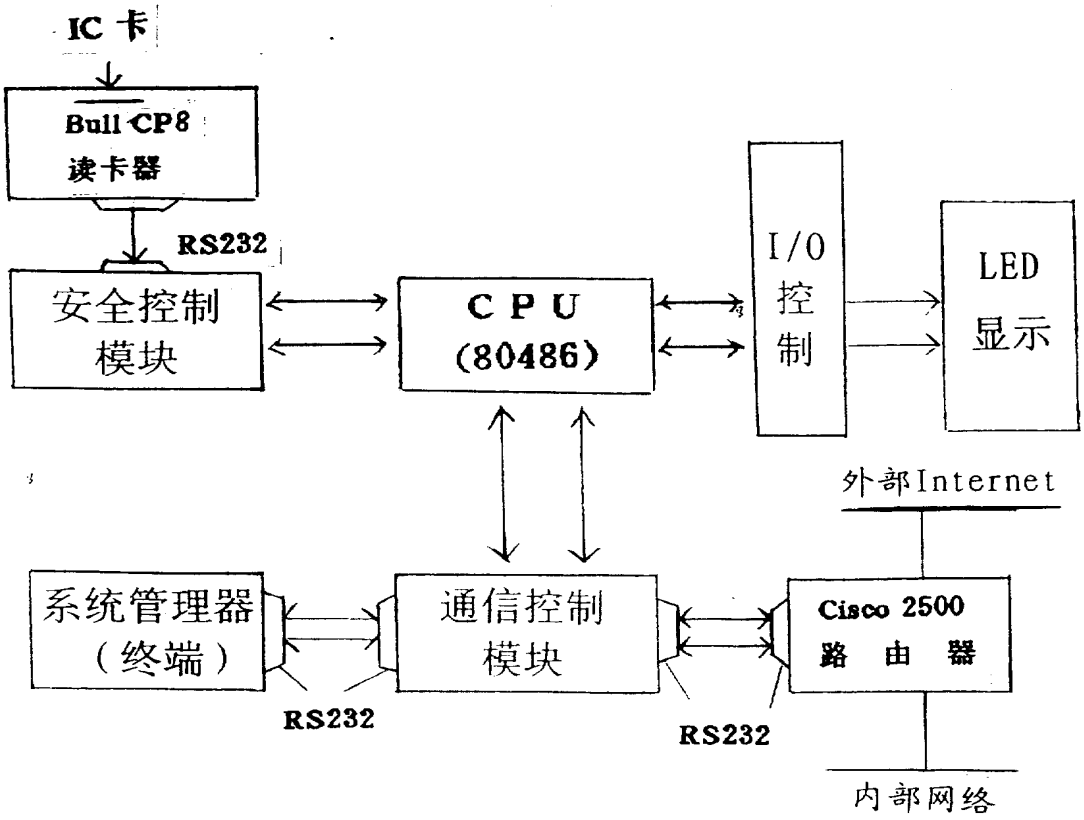

图3是本发明安全管理器实现框图

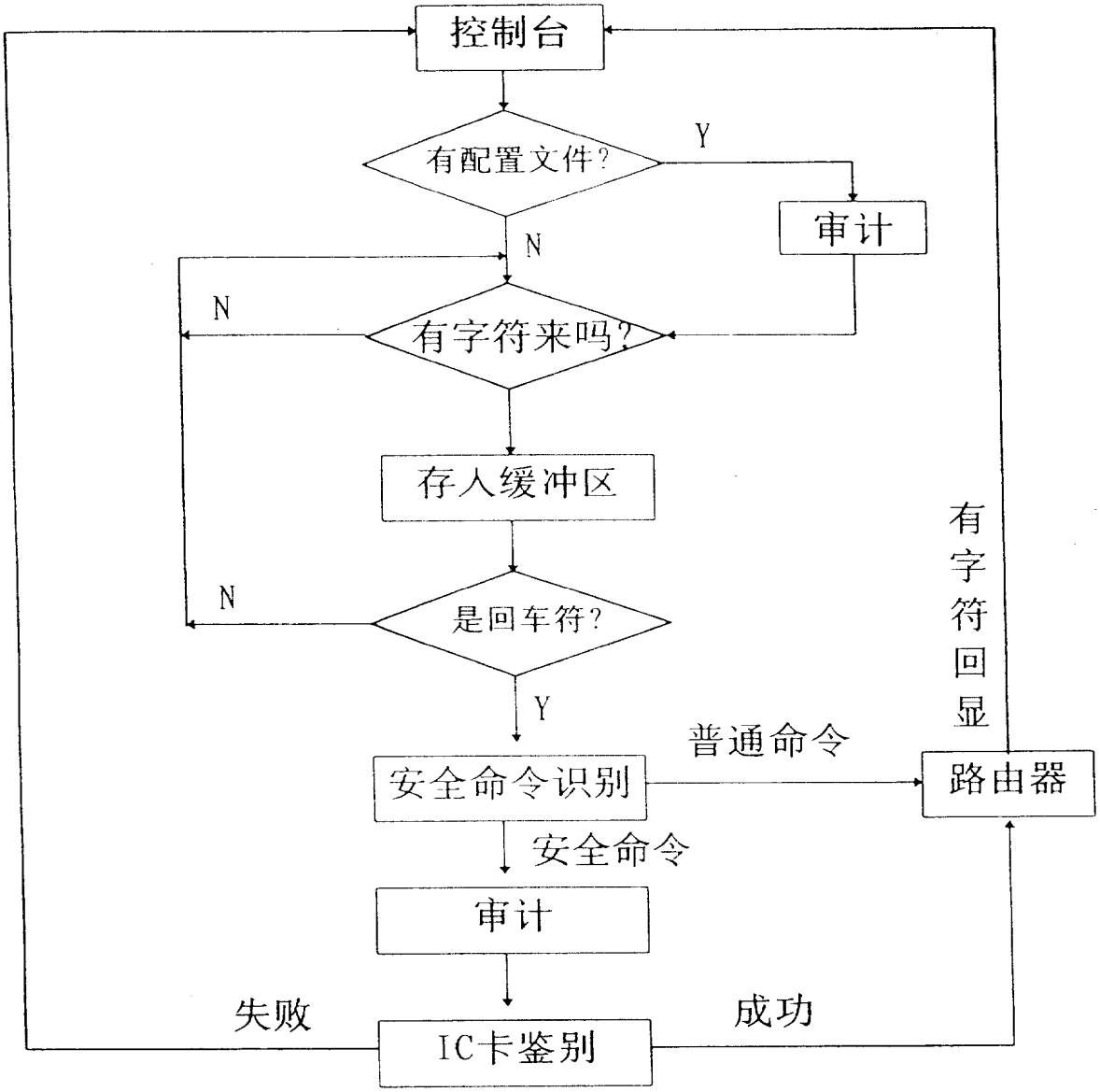

图4　　安全管理器程序流程图